Method for Prot cting Public Key Schemes from Timing, Power and Fault Attacks

ABSTRACT OF THE INVENTION

The present invention provides a method for protecting public key schemes from timing, power and fault attacks. In general, this is accomplished by implementing critical operations using "branchless" or fixed execution path routines whereby the execution path does not vary in any manner that can reveal new information about the secret key during subsequent operations. More particularly, the present invention provides a modular exponentiation algorithm without any redundant computation so that it can protect the secret key from C safe error attacks. The improved method also provides an algorithm that doesn't have a store operation with non-certain destination so that the secret key is immune from M safe error attacks.